Frank LaRose
Ohio Secretary of State

DIRECTIVE 2024-10
June 21, 2024

To: All County Boards of Elections
Board Members, Directors, and Deputy Directors

Re: Election Security for November 5, 2024, General Election (Security Directive 5.0)

SUMMARY

Since 2019, boards of elections have worked tirelessly to implement security directives that established standards for vendors, strengthened physical security requirements, and modernized cybersecurity capabilities. Implementation of these directives ensures safe elections and continues Ohioans' confidence in our democratic process. What began as a pilot project has now been successfully deployed in all of Ohio's 88 county boards of elections. Over the past several years, each of you have risen to this challenge and continued to work at a peak level of efficiency to secure our election systems in every community across the state. When it comes to election integrity and legal responsibility, we have worked hard together to establish a national reputation for election security excellence and positioned Ohio as the gold standard state. This work is ongoing because the threats change daily. Building off the success of previous directives, we continue to prioritize physical and cybersecurity while making sure you have the support and tools needed to ensure you are prepared for 2024. We are excited to collaborate and further strengthen our partnership to serve Ohioans. The below multi-faceted security strategy will help provide the redundancy required for a strong election system infrastructure. This directive works to eliminate single points of failure by providing redundant communications and ensuring back up plans are in place should a need arise. The Secretary of State Readiness grant funding is being distributed to support the requirements of this directive as well as directive 2024-09.

PHYSICAL SECURITY

Physical security of the board office is essential to protect personnel, voting equipment, voting systems, and other IT systems to maintain the confidentiality and integrity of elections. Risks, such as damage from fire or water and unauthorized physical access must be reduced whenever possible. All requirements must be completed by September 30, 2024.

A. Security of The Board Office

Boards of elections must review and comply with the security requirements outlined in Chapter 3 of the EOM. This also requires boards of elections to adopt a security policy regarding the overall security of its office. Security policies and procedures shall be audited semiannually to ensure they are up to date and being followed.

All voting equipment, along with the rooms, cases, cabinets, or cages that house the equipment, must be locked under a dual-control lock system, ensuring that any access to the equipment requires a bipartisan team.

Boards of elections are required to secure the voter registration server. Physical security provides the first line of defense to any board of elections against potential threats. Boards of elections must secure the Albert server, SIEM server, network equipment, and any other related election equipment, other than individual workstations, in a locked room at all times, accessible only to authorized personnel.

Exterior lighting for the perimeter of each board's building must be focused on entrances, exits, and the external drop box, and must be regularly inspected to ensure proper function. Adequate fire suppression equipment must be available and regularly inspected for proper functional capability. Portable extinguishers shall be visually inspected each month for physical damage, such as corrosion, leakage, or dents, and to ensure the pressure gauge is in the proper operating range, if a pressure gauge exists. Additionally, boards of election shall maintain approved video monitoring systems, for both interior bipartisan rooms and the exterior drop box. Video monitoring systems must store footage as required in Security Directive 2022-38 Technical Document and be regularly examined to ensure the system is operating as expected.

Threats of physical harm to elections officials and unauthorized entry, or attempts to gain unauthorized access to secured facilities, are security events and must be reported as soon as practical, but not longer than 24 hours, to the Secretary of State's office via [redacted].

B. MARCS Radio Emergency Interoperability

The Secretary of State's office will provide backup communications systems to each board of elections in the form of a Multi-Agency Radio Communication System, commonly referred to as MARCS radio, to promote interoperability and emergency preparedness. All boards of election must ensure adequate staff are trained on how to use the MARCS radio in case of emergency, the radio is charged and turned on during all voting periods, and the equipment is securely stored when not in use. Local law enforcement and boards of election will receive additional guidance prior to each statewide election to ensure all parties are prepared for appropriate usage, if the need arises.

CYBER SECURITY

All cyber security validations and requirements must be completed by September 30, 2024. Consistent progress towards completion will be tracked in the election security compliance checklist submitted monthly by the boards. This checklist will be reviewed during bi-weekly meetings with your cyber liaison. Boards are expected to be 50% compliant by August 1, 2024.

A. Cyber Security: Compliance with Previous Security Directives

Boards of elections must review and comply with requirements identified in Chapter 3 of the EOM and the following security directives:

- 2019-08: Security Directive 1.0
- 2020-12: Security Directive 2.0
- 2022-38: Security Directive 3.0
- 2023-16: Security Directive 4.0

B. United States Department of Homeland Security (DHS) Services

Boards of elections are designated as critical infrastructure by DHS and accordingly have access to many free DHS services.

Boards of elections must review and continue to use the Cyber Hygiene Vulnerability Scanning Service from DHS. This service provides "vulnerability scanning of Internet-accessible systems for known vulnerabilities on a continual basis as a no-cost service. As potential issues are identified, DHS notifies impacted customers so they may proactively mitigate risks to their systems prior to exploitation. The service incentivizes modern security practices and enables participants to reduce their exposure to exploitable vulnerabilities."

Each board of elections is required to request the following services, and if enrolled, agree to the following services when an invitation from DHS is received:

- **Phishing Campaign Assessment.** This assessment is a "no cost six-week engagement that evaluates an organization's susceptibility and reaction to phishing emails of varying complexity."
- **Risk and Vulnerability Assessment.** This onsite assessment gathers data and combines it with national threat and vulnerability information to detect vulnerabilities in network security. After completing the assessment, DHS provides a final report with its findings and recommendations for improving network security controls.
- **Remote Penetration Testing.** DHS provides this service remotely to identify vulnerabilities in externally accessible systems. After completing testing, DHS provides a final report with its findings and recommendations.
- **Validated Architectural Design Review.** This review is designed to develop a detailed representation of the communications and relationships between devices to identify anomalous communication flows. Following the review, a participating organization will receive a report that includes discoveries and recommendations for improving organizational operations and cybersecurity.
- **Web Application Scanning.** This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations.

Election officials can obtain information on these resources and services by contacting DHS at: CISAServiceDesk@cisa.dhs.gov.

C. Elections Infrastructure Information Sharing

Boards of elections must review their personnel information with the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) and make any necessary updates to ensure that the appropriate personnel at the board of elections and/or county IT receive and review emails. New board and staff members must register at https://learn.cisecurity.org/ei-isac-registration, and boards must notify the EI-ISAC of contact information changes via email to elections@cisecurity.org.

D. Vulnerability Disclosure Program

A Vulnerability Disclosure Program (VDP) is a formalized process to receive, validate, remediate, and communicate vulnerability information identified by security researchers on specific technology systems. VDPs have proven successful in many industries, from the largest tech companies to small governments. They can be an effective and efficient way for an organization to improve its security posture.

The EI-ISAC offers a vulnerability disclosure program to all boards of elections at no cost. Boards of elections are highly encouraged to enroll in this free program. To enroll in this service please email elections@cisecurity.org and copy dlessard@ohiosos.gov.

E. Ohio Secretary of State Provided Services

This section of the Directive outlines the services that the Secretary of State's office will continue to provide in order to support Ohio's secure elections infrastructure at no cost to the county boards of elections.

1. Cyber Liaisons

The Secretary of State's office will continue to engage cybersecurity professionals to assist the county boards of elections with their IT support needs. Currently cyber liaisons are deployed to each region of Ohio: Northeast, Northwest, Southeast, and Southwest. The cybersecurity liaisons promote best practices to further improve the board's cybersecurity and complement the board's current IT support. For example, cyber liaisons assist boards and local IT support with tools, software or hardware integration, software and patch management support, network analysis review, incident response planning and exercising, tier one incident management forensic collection support, and general engineering technical assistance.

2. Network Intrusion Detection

Boards of elections must continue using the Albert Intrusion Detection Monitoring service (Albert). The Albert must be configured to monitor the board of elections' network traffic and may also be used to monitor the overall county network traffic so long as the board of elections' network traffic is included in that monitoring. Boards should review and update their incident response plan related to Albert alerts with their county cyber liaison.

3. Security Information and Event Management (SIEM)

Boards of elections must continue using the SIEM Logging service. All boards of elections network systems must be configured to log system events to the SIEM. Other county log events may also be sent to the SIEM, so long as the board of elections system events are continuously monitored. Server refresh is a reimbursable cost under the above-mentioned grant.

4. Endpoint Detection and Response (EDR) Solution

Boards of elections must continue to use the EDR solution provided by the Secretary of State's Office. EDR solutions protect systems more effectively than the traditional anti-virus

products by scanning for known bad behavior and characteristics of malicious actors, rather than looking only for bad files like traditional anti-virus software.

If the board of elections is unable to implement the Secretary of State's supplied EDR solution, the board must document how their current EDR solution meets the Secretary of State's requirements.

5. Malicious Domain Blocking and Reporting

The Secretary of State continues to provide a malicious domain blocking and reporting service (MDBR) for all county boards of elections. This service blocks access to malicious websites, helps stop malware from connecting to known command-and-control infrastructure, and complements the Albert and SIEM services. Each board of elections must maintain the service and continue using this malicious domain blocking service or an approved equivalent. While the boards of elections must utilize this service, the entire county is encouraged to take advantage of this service at no cost.

F. Technical Controls

1. Board of Elections Websites

Boards of elections must ensure that their websites can withstand the heavy traffic associated with a Presidential general election. Boards and their vendors must continue to utilize TLS/SSL certificates for any publicly facing or internal web-based applications (e.g., the county board of elections website) and ensure that its existing certificates do not expire.

All boards of elections websites, including vendor provided systems for election and voter related information, must be protected by a web application firewall and content delivery services.

2. Vulnerability Management

The Secretary of State's office will continue to provide an authenticated vulnerability scanning service to the Boards of Elections at no cost to the boards. Boards of elections must conduct authenticated vulnerability scans at least once a week. Boards must retain evidence that these scans are completed and acted upon for at least one year.

Boards of elections must remediate vulnerabilities in network-connected systems in a timely manner. Critical and high vulnerabilities must be remediated within 15 calendar days of initial detection; all other vulnerabilities must be remediated within 30 calendar days of initial detection. In order to meet the specified timelines, boards of elections are encouraged to utilize a patch management solution.

3. Approved Operating Systems

All computer operating systems must be supported by their manufacturer and receive regular security updates.

G. Cybersecurity Training

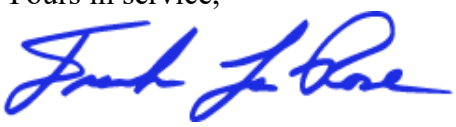
Each board member and employee must complete an approved security awareness training course annually and whenever a new board member or employee starts with the board of elections. A copy of the certificate of completion or a report from the training system must be provided to the Secretary of State's office within 30 days of completion via email to HAVAGrant@OhioSoS.gov. The Secretary of State's office will continue to provide the training at no cost to the boards of elections. Additionally, boards are required to participate in tabletop exercises, as outlined in the EOM. The Secretary's office will make tabletop opportunities available including but not limited to the 2024 US DHS CISA's "TTX The Vote" national exercise, the Ohio Secretary of State hosted Regional Readiness Workshops, and other state and federally supported exercises.

H. Resilience

The board of elections voter registration server and any data processed by the board of elections must be backed up daily. Other critical systems, such as file servers, must be backed up at least once a week. These backups must be stored in a secure off-site off-network location. Boards must retain copies of backups for at least three weeks. At a minimum, boards must annually test the backup to ensure that the voter registration server and other critical systems can be fully restored using the off-site backup.

Working together we can ensure Ohio is prepared for the 2024 election and that Ohioans have confidence in the election outcome.

Yours in service,



Frank LaRose
Ohio Secretary of State